DSTEP — DES Step — DSTEP

Format:

```
DES  Dest, Src1, Src2
```

Encoding:

110111	11	Dest	Src1	100010	Src2
6	2	6	6	6	6

Description:

Perform one round of the DES (Data Encryption Standard) algorithm. Sixteen rounds of this instruction are needed to perform the body of the DES function on 64 bits of data. *Src1* is the 64 bit input to the DES round, *Src2* is the 48 bit key for the round being executed. Note that each of the 16 rounds of DES requires a different subkey based on the original key. The 16 subkeys can be computed all at one time whenever the key becomes known for the data.

This instruction may be used to both encrypt and decrypt data depending on the order in which the 16 keys are applied to the data.

Operation:

Src1 contains the 64 bit data in byte-interleaved form.

Src2 contains the 48-bit subkey where each byte of *Src2* contains six bits of the key in the least-significant bits of each byte.

The DSTEP instruction performs one round of DES, which is defined to be

- The expansion permutation
- Combine with subkey
- S-box substitution
- P-box permutation
- Combine right and left halves

Upon completion, *Dest* contains the byte-interleaved result ready for input to the next round of DES.

The byte-interleaved forms of *Src1* and *Dest* look like the following:

```
              MSb                                   LSb
              ---------------------------------------
Byte 7 (MSB): L31  L30  L29  L28  L27  L26  L25  L24
Byte 6      : R31  R30  R29  R28  R27  R26  R25  R24
Byte 5      : L23  L22  L21  L20  L19  L18  L17  L16
Byte 4      : R23  R22  R21  R20  R19  R18  R17  R16
Byte 3      : L15  L14  L13  L12  L11  L10  L9   L8
Byte 2      : R15  R14  R13  R12  R11  R10  R9   R8
Byte 1      : L7   L6   L5   L4   L3   L2   L1   L0
Byte 0 (LSB): R7   R6   R5   R4   R3   R2   R1   R0
Where:
L31 is the MSb of L.
L0  is the LSb of L.
R31 is the MSb of R.
R0  is the LSb of R.
```

Flags Affected:

None.

Execution Exceptions:

State 104

None.

Notes:

For more information regarding the DES algorithm, see chapter 12 of "Applied Cryptography", Second Edition, by Bruce Schneier. 1996. *Note: in the "Applied Cryptography" book, bit 1 is the MSB.*

A Technical Application Note (containing an optimized code example) is available in CVS at `/tapestry/examples/applications/des`.